Doc Code: AP.PRE.REQ

PTO/SB/33 (07-05)
Approved for use through xx/xx/200x. OMB 0651-00xx
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

PRE-APPEAL BRIEF REQUEST FOR REVIEW	Docket Number (Optional) S0193.0011	
	Application Number 10/735,517-Conf. #1592	Filed December 11, 2003
	First Named Inventor Gernot Eckstein et al.	
	Art Unit 2131	Examiner A. R. Sheikh

Applicant requests review of the final rejection in the above-identified application. No amendments are being filed with this request.

This request is being filed with a notice of appeal.

The review is requested for the reason(s) stated on the attached sheet(s).
Note: No more than five (5) pages may be provided.

I am the

☐ applicant /inventor.

☐ assignee of record of the entire interest.
See 37 CFR 3.71. Statement under 37 CFR 3.73(b) is enclosed. (Form PTO/SB/96)

☒ attorney or agent of record.
Registration number 38,395

☐ attorney or agent acting under 37 CFR 1.34.
Registration number if acting under 37 CFR 1.34. _____

Laura C. Brutman
Signature

Laura C. Brutman
Typed or printed name

(212) 277-6592
Telephone number

November 13, 2007
Date

NOTE: Signatures of all the inventors or assignees of record of the entire interest or their representative(s) are required. Submit multiple forms if more than one signature is required, see below*.

☐ *Total of 1 forms are submitted.

ATTACHMENT TO PRE-APPEAL BRIEF REQUEST FOR REVIEW

Claims 1-8 have been examined with all claims rejected based on prior art. More specifically, claims 1-5 and 8 remain rejected under 35 USC 102(e) as being anticipated by Kash et al. (U.S. Patent No. 6,515,304; hereinafter "Kash"), and claims 6, 7, 9, and 10 are rejected under 35 USC 103(a) as being unpatentable over Kash in view of Klughart et al. (U.S. Patent No. 6,396,137; hereinafter "Klughart"). Applicant respectfully traverses this rejection for the reasons set forth below.

The claimed invention is concerned with the prevention of unauthorized external access to the operation of an integrated digital circuit. More specifically, the invention is concerned with counter-measures against so-called sidechannel attacks, which are performed by unauthorized parties for analyzing integrated digital circuits, for example, for analyzing coding algorithms performed by cryptocoprocessors.

Typically, integrated circuits are implemented as synchronous circuits, which operate on the basis of a clock signal. It is a standard approach in the prior art to introduce random wait states into the operation of such synchronous circuits to thus randomly delay timing of operation of such synchronous circuits. In a typical approach, an external clock is internally randomly delayed within the synchronous circuit to thus randomly postpone the occurrence of the internal operations along with the random delay of the clock to thus make it more difficult for unauthorized persons to analyze the internal operations.

Claim 1 refers to "an asynchronous circuit." In the Advisory Action, the Examiner continues to uphold his technically incorrect interpretation of the Kash circuit as an "asynchronous circuit." The term "asynchronous circuit" has a clear technical meaning to one of ordinary skill in the present technical field, i.e., to an electrical engineer. Applicant submitted along with the September 24, 2007 Response as evidence, a definition of an asynchronous circuit as provided by the Encyclopedia "Wikipedia." An asynchronous circuit is a self-timed circuit which is not governed by any clock signal, or which does not operate according to a clock signal. Therefore, an asynchronous circuit is not a circuit operating in accordance with a clock and which generates due

to some delays some operations which are not directly correlated to a time-specific event, such as a clock.

Therefore, one skilled in the present field would clearly consider the circuit of Kash to be a synchronous circuit as the same is driven by clock timing signals. This is also true for the Fig. 6 embodiment of Kash in which the external clock is randomly delayed in order to generate a jittered internal chip clock which forms the basis of the operations of the internal clocked circuit. Thus, the internal circuit is a synchronous circuit governed by a clock, although this clock is randomly delayed relative to an external clock. In other words, the jitter or random delay of the clock does not change the nature of the circuit, namely to be a synchronous circuit. As outlined in the September 24, 2007 Response, the Kash circuit operates in synchronism with the jittered or randomly delayed internal clock.

Referring now to the claim element concerning the variation of the electric supply voltage, the Examiner refers to the text portions of column 3, line 66, to column 4, line 3. However, these text portions of the reference do not refer to the Fig. 6 embodiment of Kash. Rather, the same refers to a technology used for facilitating the non-destructive reverse engineering of a circuit by monitoring the modulation of a reflected light beam by parts of active elements or devices in the integrated circuit. See column 3, lines 51-53. A time varying voltage across an interface in the integrated circuit produces a time-varying modulation of reflectivity from the interface that can be measured and used to obtain information on time varying voltages. See column 3, line 66, to column 4, line 3. This technique serves for analyzing the operation of internal parts of an integrated circuit by a reflected light beam and has nothing to do with the variation of a supply voltage of a circuit. Thus, the Examiner's implicit argument that the time variation can be derived from column 3, line 66, to column 4 line 3, of Kash is based on a technical misunderstanding on the Examiner's part.

The Examiner is also incorrect when stating that the second reference to Klughart discloses an integrated circuit that operates in an asynchronous manner which is equivalent to Applicant's invention. Klughart also does not deal with any asynchronous circuits. Rather, this reference

establishes an additional security against reverse engineering performed by third parties (see column 34, lines 42-48). Klughart teaches arranging layers of metal and specific semiconductor materials above switches and regulators in integrated circuits to thus prevent unauthorized access by third parties to the operation of these switches and regulators (see column 34, lines 49-64).

As outlined in the September 24, 2007 Response, the Examiner's allegations that Klughart discloses an asynchronous circuit are not supported by Klughart. The Examiner refers to column 16, lines 49-53. This section of the description does not deal with any asynchronous circuits at all.

The Examiner further refers to column 37, lines 30-35. As previously outlined, this section refers to a switching regulator/power converter which asynchronously modulates its pulse width or frequency in order to compensate for changing the load requirements. However, this is not an asynchronous circuit. Therefore, Klughart does not deal with any asynchronous circuit. Moreover, Klughart does not teach or suggest varying the supply voltage of any asynchronous circuit.

Applicants respectfully submit that pending claims are patentable over the applied references. Favorable consideration and a Notice of Allowance are earnestly solicited.